Introduction to IPSec

Overview of Presentation

- Introduction
  - The Internet Model and Threats
  - Solutions Possible
  - Security Measures at Various Layers
  - IPsec: security at network layer
- How IPsec works
  - IPsec model
  - Authentication Header
  - Encapsulating Security Payload
  - Internet Key Exchange
- Limitations of IPsec
- Conclusions

Introduction

- Original Design Model for Internet
  - The model of Internet was made for a more benign environment like academia
  - All data on Internet was free to all and anyone could share or modify the data
  - Since the some etiquette was being observed by the limited Internet community, security was hardly an issue
  - Internet has grown beyond academia

Introduction (contd.)

- In present scenario, Internet enables instant on-demand business by
  - Establishing communication links with suppliers and business partners
  - By eliminating the need for costly wide area network dedicated lines
  - Enabling remote access to corporate networks using many available Internet service providers
- One of the main stumbling blocks to achieve these benefits is lack of security (besides, reliability, quality of service among others)

Internet Threats

- The varied nature of Internet users and networks has brought the security concern
- To ratify the fears several threats have surfaced, such as,
  - Identity spoofing
  - Denial of service
  - Loss of privacy
  - Loss of data integrity
  - Replay attacks

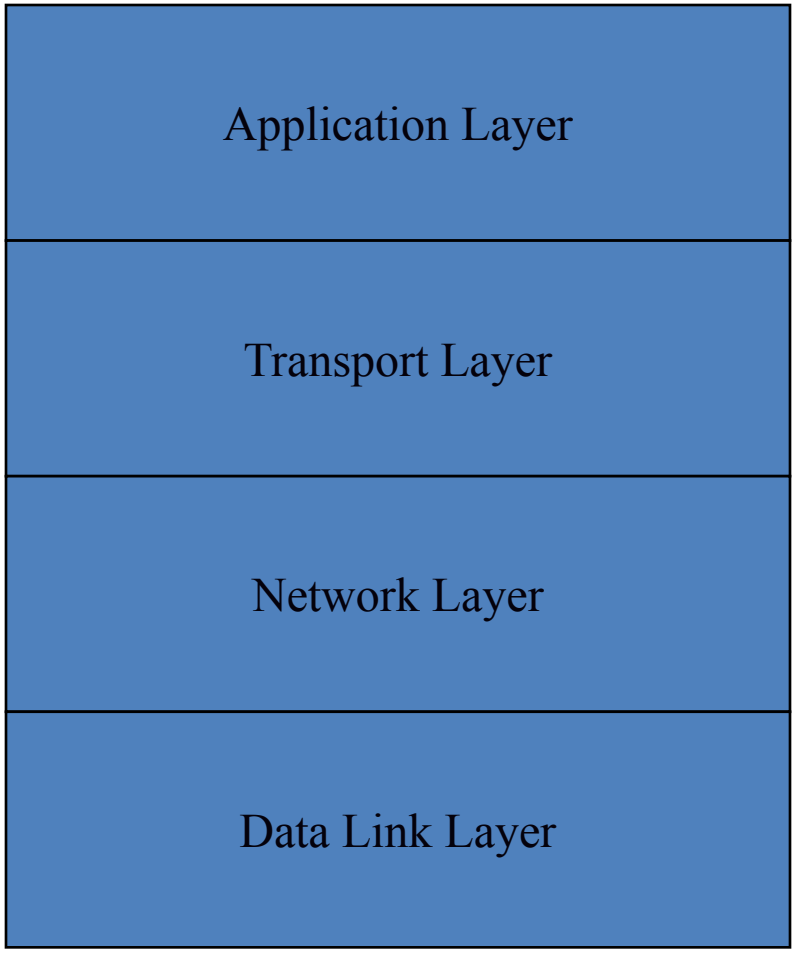
Internet Threats (contd.)

- Identity spoofing
  - Executing transactions by masquerading
- Denial of service
  - Preventing a service provider by flooding with fake requests for service
- Loss of privacy
  - Eavesdropping on conversations, database replies etc
- Loss of data integrity
  - Modifying data in transit to disrupt a valid communication
- Replay attacks
  - Using older legitimate replies to execute new and malicious transactions

Solutions to the Problems

- Confidentiality
  - If data is encrypted intruders cannot observe
- Integrity
  - Modification can be detected
- Authentication
  - If devices can identify source of data then it is difficult to impersonate a friendly device
  - Spoofing , replay attacks and denial of service can be averted
- The question is where should such a solution be implemented in the protocol stack?

Security Measures at Different Layers



PGP, Kerberos, SSH, S/MIME

SSL/Transport Layer Security (TLS)

IPsec

Hardware encryption

Security Measures at Different Layers (contd.)

- Application Layer Security
  - Implemented as a User Software
  - No need to modify operating system or underlying network structure
  - Each application and system requires its own security mechanisms
- SSL/TLS (transport layer security) is implement as user-end software, and is protocol specific
- Link layer security
  - Implemented in hardware
  - Requires encryption decryption between every link
  - Difficult to implement in Internet like scenario

IPsec: Security at IP Layer

- IPsec is a framework of open standards developed by IETF (www.ietf.org, rfc's 4301-4308)
- IPsec is below transport layer and is transperant to applications
  - IPsec provides security to all traffic passing through the IP layer
- End users need not be trained on security mechanisms, issued keys or revoked
- IPsec has the granularity to provide per-user security if needed

IPsec: Security at IP Layer (contd.)

- IPsec has additional advantages of protecting routing architecture
  - IPsec can assure that a router advertisement is from an authorized router
  - A routing update is not forged
  - A neighbor advertisement comes from an authorized router

IPsec Services

- Access control
- Connectionless Integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality
- Limited traffic flow confidentiality

SA(security association) Parameters

- Sequence Number Counter
- Sequence Counter Overflow
- Anti-Replay Window
- AH Information
- ESP Information
- Lifetime of SA
- IPSec Protocol mode –Tunnel, Transport
- Path MTU

IPsec components

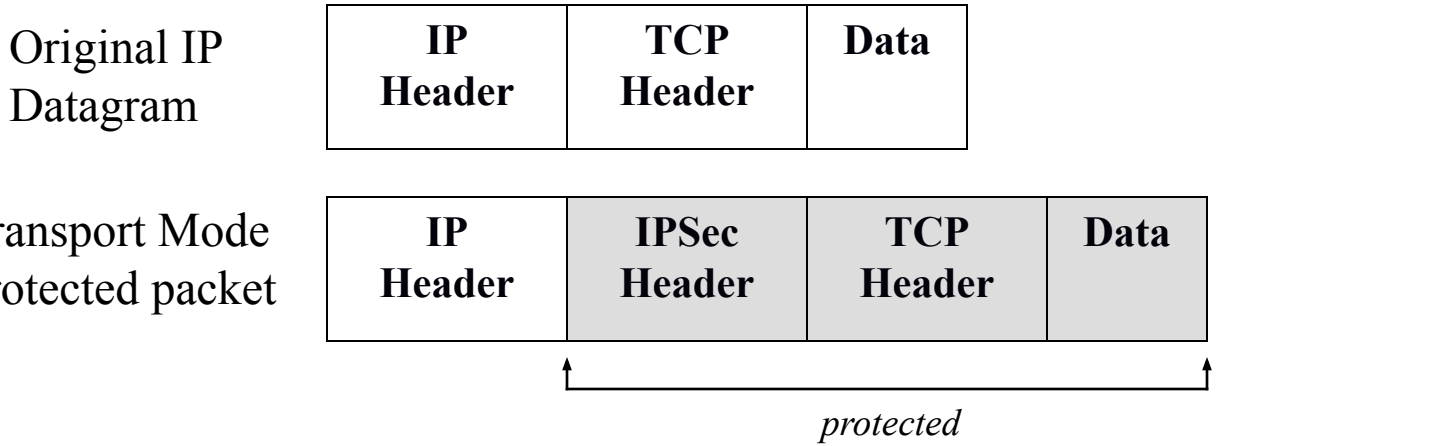
- IPsec consists of two important protocol components
  - The first, defines the information that needs to be added to the IP packet to achieve the required services. These are classified further as Authentication Header and Encapsulating Security Protocol
  - The second, Internet Key Exchange, which negotiates security association between two peers and exchanges keying material

IPsec Modes

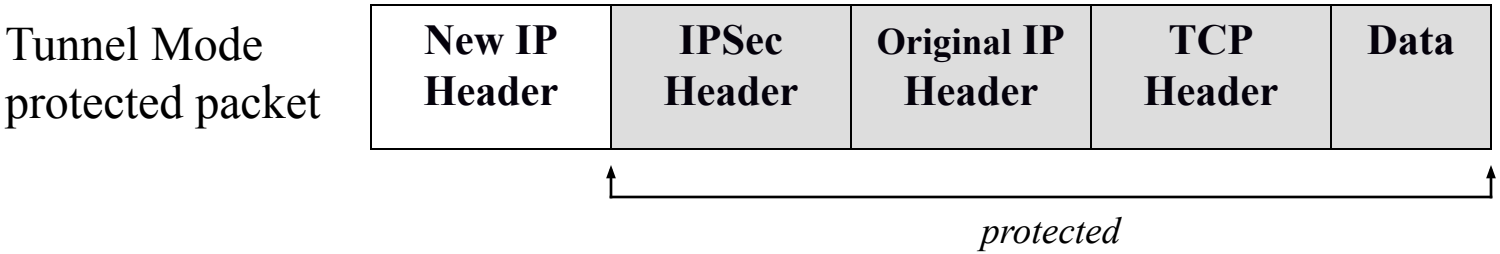
- IPsec can operate in two modes
  - Transport Mode
    - Only IP payload is encrypted
    - IP headers are left in tact
    - Adds limited overhead to the IP packet
  - Tunnel
    - Entire IP packet is encrypted
    - New IP headers are generated for this packet
    - Transparent to end-users

IPsec modes (contd.)

- Transport Mode: protect the upper layer protocols



- Tunnel Mode: protect the entire IP payload



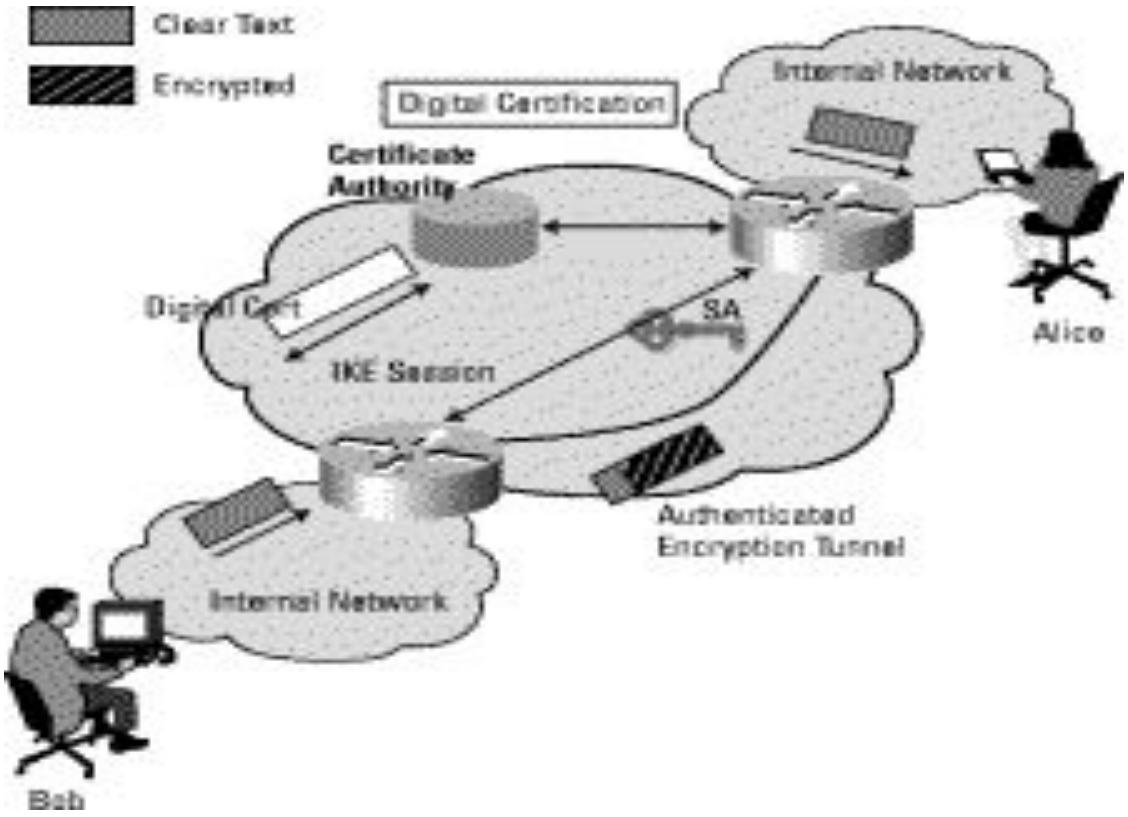
Authentication Header

- This information is added to the header to provide the following services:
  - Access control, connectionless integrity, data origin authentication, rejection of replayed packets
  - Information added are:
    - Sequence number (32-bit)
    - Integrity check value (variable, multiple of 32-bits)

Authentication Header (contd.)

- Anti-replay attacks
  - Range of sequence numbers for session is 2^{32}-1
  - Sequence numbers are not reused
- Integrity Check Value (ICV)
  - Keyed MAC algorithms used: AES, MD5, SHA-1
  - MAC is calculated over immutable fields in transit (source/dest. addr, IP version, header length, packet length)

IKE(internet key exchange) and IPsec



Limitations

- Security implemented by AH and ESP ultimately depends on their implementation
- Operating environment affects the way IPsec security works
- Defects in OS security, poor random number generators, misconfiguration of protocols, can all degrade security provided by IPssec.

Conclusions

- IPsec provides a method for creating secure private networks over public networks
- Applications, operating systems need not be changed
  - Implementation can be limited to secure gateways
- Several products based on IPsec are commercially deployed
- Users can even enable and use IPsec on their machines

PGP and S/MIME

- **Pretty Good Privacy (PGP)**

- PGP is an open-source software package that is designed for email security.
- It provides the basic or fundamental needs of cryptography. In this multiple steps are taken to secure the email, these are,

  - **Confidentiality**
  - **Authentication**
  - **Compression**
  - **Resemble**
  - **Segmentation**
  - **E-mail compatibility**

- **Secure/Multipurpose Internet Mail Extension (S/MIME)**
- S/MIME is a security-enhanced version of Multipurpose Internet Mail Extension (MIME). In this, public key cryptography is used for digital signs, encrypting, or decrypt email.
- The user acquires a public-private key pair with a trusted authority and then makes appropriate use of those keys with email applications.

Difference Between PGP and S/MIME

S.NO	PGP	S/MIME
1.	It is designed for processing plain texts	While it is designed to process email as well as many multimedia files.
2.	PGP is less costly as compared to S/MIME.	While S/MIME is comparatively expensive.
3.	PGP is good for personal as well as office use.	While it is good for industrial use.
4.	PGP is less efficient than S/MIME.	While it is more efficient than PGP.
5.	It depends on user key exchange.	Whereas it relies on a hierarchically valid certificate for key exchange.
6.	PGP is comparatively less convenient.	While it is more convenient than PGP due to the secure transformation of all the applications.

7.	PGP contains 4096 public keys.	While it contains only 1024 public keys.
8.	PGP is the standard for strong encryption.	While it is also the standard for strong encryption but has some drawbacks.
9.	PGP is also be used in VPNs.	While it is not used in VPNs, it is only used in email services.
10.	PGP uses **Diffie hellman digital signature**.	While it uses **Elgamal digital signature**.
11.	In PGP Trust is established using Web of Trust.	In S/MIME Trust is established using Public Key Infrastructure.
12.	PGP is used for Securing text messages only.	S/MIME is used for Securing Messages and attachments.
13.	Their is less use of PGP in industry .	While S/MIME is widely used in industry.